

Claims

1. A modular component for use in conjunction with a protocol stack of a voice over internet protocol (VoIP) terminal, comprising:

- a security manager;
- a security stack interface (SSA) for interfacing between said security manager and a protocol manager of said protocol stack;
- a security terminal interface (SST) for interfacing between said security manager and an application layer;
- a security media interface (SSM) for interfacing between said security manager and a media controller; and
- a security manager application interface (SMA) for interfacing between said security manager and a security application (PGP) outside said stack.

2. The modular component of claim 1, wherein said security manager comprises a state machine having an idle state and a wait for authorization state.

3. The modular component of claim 2, wherein a transition to said wait authorization state from said idle state occurs in response to an unauthorized invitation received and signaled from and to an initiating remote device wherein a transition from said wait authorization state to said idle state occurs in response to an authorized invitation.

4. A session initiation protocol (SIP) signaling stack for a voice over internet protocol (VoIP) terminal device, said stack having an application interface and a media interface to a telephony application and having a protocol interface to a network layer, said stack comprising:

- an SIP manager having said application interface and a media controller having said media interface to said telephony application and said protocol interface between said network layer and both said SIP manager and said media controller; and
- a security manager having a plurality of interfaces to said SIP manager, said telephony application, and to said network layer.

5. The SIP stack of claim 4, wherein said plurality of interfaces includes:

- (i) a security stack interface (SSA) between said SIP manager and said security manager;
- (ii) a security terminal interface (SST) between said telephony application and said security manager;
- (iii) a security media interface (SSM) between said security manager and said media controller;
- (iv) a security manager application interface (SMA) between said security manager and a security application (PGP) outside said stack.

6. Method, comprising the steps of:

sending an invite signal from a session initiation protocol (SIP) stack of a sending terminal to a remote user agent (UA);

receiving an unauthorized signal (401_Unauthorized) at said SIP stack from said remote UA indicating authorization is required;

providing an indication signal (got_401_unauthorized) from said SIP stack to a security manager module of said sending terminal indicative of receipt of said unauthorized signal;

providing an authenticate signal (send_www_authenticate) with required information and authorization header field from said security manager module to said SIP stack;

calling encryption and authorization function requests from said SIP stack to said security manager;

encrypting and authorizing said required information; and

sending an authorized invite signal from said SIP stack to said remote UA.

7. Method, comprising the steps of:

receiving an invite signal from a remote user agent (UA) at a session initiation protocol (SIP) stack of a receiving terminal;

providing a signal indicative of receipt of said invite signal from said SIP stack to a security manager module of said receiving terminal for checking security parameters of said invite signal;

providing an authenticate signal (send_www_authenticate) from said security manager to said SIP stack;

sending an unauthorized signal (401_unauthorized) from said SIP stack to said remote UA;

5 receiving an authorized invite signal from said remote UA to said SIP stack;

providing a request to authenticate said authorized invite signal to said security manager module;

checking parameters of said authorized invite signal by said security manager module; and

10 providing an authentication signal from said security manager module to said SIP stack indicative of said step of checking.

8. A telecommunications system, comprising:

15 a sending terminal for sending an invite signal from a session initiation protocol (SIP) stack of a sending terminal; and

a receiving terminal responsive to said invite signal for providing a signal indicative of receipt of said invite signal from said SIP stack to a security manager module of said receiving terminal for checking security parameters of said invite signal, wherein said security manager provides an authenticate signal to said SIP stack and said SIP then sends an unauthorize signal to said sending terminal in the presence of an unauthorized invite signal from said sending terminal, wherein said SIP stack of said sending terminal is responsive to said unauthorized signal from said receiving terminal indicating authorization is required, and wherein said sending terminal provides an indication signal from said SIP stack of said sending terminal to a security manager module of said sending terminal indicative of receipt of said unauthorize signal, wherein said security manager provides an authenticate signal with required information and authorization header field to said SIP stack of said sending terminal, wherein said SIP stack of said sending terminal sends an authorized invite signal to said receiving terminal, wherein said receiving terminal receives said authorized invite signal from said sending terminal at said SIP stack of said receiving terminal, wherein said SIP stack provides a request to authenticate said authorized invite signal to said

